Tutorial

Enterprise Wireless Mobility

Abstract

Introduction

Two of the hot areas in information technology are wireless networks and security for all types of networks. Cisco has recognized this in the new blueprint for the CCIE R&S Written Exam (350-001). The last topic on this list is titled Enterprise Wireless Mobility. Under this topic, the following are listed as possible sources for questions:

- Standards
- Hardware
- SWAN
- RF Troubleshooting
- VoWLAN
- Products

The majority of Cisco's efforts are contained in the SWAN initiative. The SWAN (Structured Wireless-Aware Network) approach integrates the management of the wireless and wired parts of the network into a seamless whole. As part of this, all of the hardware and products from Cisco will need to support this, which is why they are listed. These hardware devices and the software that runs on them must support the industry standards when they exist and Cisco additions when there is no standard. VoWLAN (voice over wireless local area networks) is the ability to use the wireless network for voice as well as data. Radio frequency (RF) troubleshooting will be dealt with in a separate tutorial. This tutorial begins with SWAN because SWAN contains most of the other elements in one form or another.

SWAN

As Cisco says about SWAN:

> "The Cisco Structured Wireless-Aware Network (SWAN) provides the framework to integrate and extend wired and wireless networks to deliver the lowest possible total cost of ownership for companies deploying wireless LANs (WLANs). Cisco SWAN extends 'wireless awareness' into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations have come to expect from their wired LANs.
>
> From small businesses to large-scale enterprise multinational companies; within WLAN campus deployments or branch offices; at universities; in retail, manufacturing, or healthcare industries; or at hot spot locations, Cisco SWAN reduces overall operational expenses by simplifying network deployment, operations and management. With Cisco SWAN, several, hundreds, or thousands of central or remotely located Cisco Aironet Series access points can be managed from a single management console. Cisco SWAN's flexibility allows network managers to design networks to meet

their specific needs, whether implementing a highly integrated network design or a simple overlay network."

Cisco shows this as an integrated approach with elements at all three layers of the Cisco network design model: core, distribution, and access.

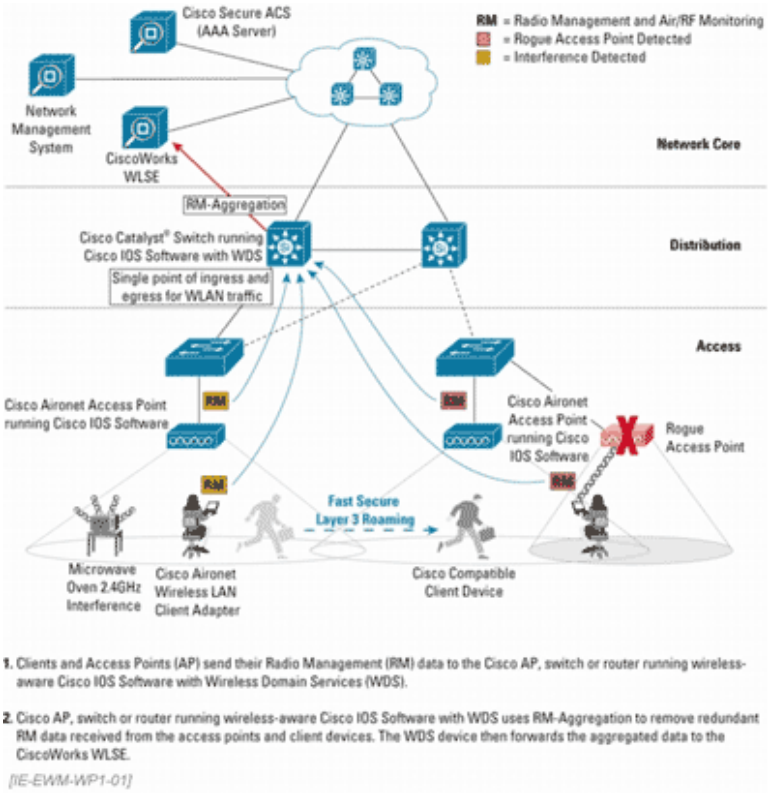


Figure 1. The Components of SWAN

Cisco lists the benefits of SWAN as:

- Easier deployment through assisted site surveys
- Ability to manage from a single location a few to thousands of access points located locally or remotely
- Integrated security
- Enhanced roaming ability
- Radio interference troubleshooting

To achieve the full benefits of SWAN, four components must be installed. These are:

- Cisco Aironet access points
- The Wireless LAN Solution Engine (WLSE)
- An IEEE 802.1x authentication server
- Client devices that support the Cisco Wireless Extensions

Cisco Aironet Access Points

There is an extensive line of Aironet access points and client adaptors. Because the blueprint has a separate topic for hardware, the details of these devices are discussed later in this tutorial. For SWAN compatibility, these access points must support the wireless features in the Cisco IOS.

WLSE

A significant part of the SWAN initiative is the Wireless LAN Solution Engine (WLSE). The WLSE is a combination of hardware and software in the form of a 1U Linux-based appliance that is placed in the network operations center. It is then connected to a Cisco Catalyst switch. The software allows a single management platform to control thousands of access points through a single web-based interface. For example, Version 2.9 can support up to 2,500 access points in a single domain. More can be supported through multiple domains.

WDS

WLSE interoperates with the features provided by the Wireless Domain Services (WDS) software. WDS is a set of Cisco IOS features specifically developed for wireless devices. It provides the necessary software support for client mobility, deployment, and management. Unlike the other components of SWAN, WDS can reside in one of several locations, depending on the size of the wireless network. At this time, WDS runs on the Cisco Aironet 1230 AG, 1200, 1130 AG, and 1100 Series access points as well as the Catalyst 6500 Series WLSM-equipped switches. WDS can operate in these other devices because it uses its own control and data planes. Therefore, data handling rates are unaffected. Beginning in 2005, the features of WDS will be added to more devices such as routers and switches.

In the SWAN-enabled environment, WDS aggregates radio management information collected from access points and client adaptors and sends this information to the WLSE where it is used to manage, monitor, and control the RF environment. For interference and security management, the WDS takes the RF measurements made by the access points and forwards them to the WLSE for analysis. Based on this information, the WLSE can detect rogue access points, can detect interference from other devices, can provide assisted site surveys, and can adjust the devices for optimal coverage.

Fast Secure Roaming requires WDS because it eliminates the need for a reauthentication by an authentication server. This allows the speed of reassociation required for real time applications. WDS must be able to converse with the authentication server and the access points for this to function.

WDS is a required component for full SWAN functionality. For deployments that use access point-based WDS, at least one WDS AP per subnet is required for RF management of that subnet. For deployments that use the Catalyst 6500 Series switch, access points located in different subnets can be supported by a single WLSM-enabled Catalyst 6500 Series switch.

The configuration of the WDS depends on the device on which it is running.

WLSM

The Wireless LAN Services Module (WLSM) is a card that is placed in a Catalyst 6500 Series switch.

Figure 2. The Wireless LAN Services Module

The WLSM provides a common aggregation point for the data the access point radio management functions prepare for use by the WLSE. It provides a central key management system to help ensure security of client roams. It also provides authentication for 1100 and 1200 Series access points. Finally, it assists in client mobility management, such as layer 2 and 3 roaming.

This module is required for key components of SWAN such as:

- Layer 3 roaming

- Establishing different groups of users. Each group can be managed with its own set of access controls. For example, an employee can be provided with more access than a guest has. Up to 16 groups are currently supported.
- Extending the 6500 switch's ability to provide denial of service, access control list, network intrusion detection, and VPN services to the wireless -- not just the wired -- network.
- Providing the ability to configure new devices
- Providing a single control point for all wireless traffic

For full functioning, this card requires the Supervisor Engine 720. The combination of the Catalyst 6500, the Supervisor 720, and the WLSM is quite expensive. This is not a solution for a small to medium size operation.

Configuration of the WLSM is straightforward. After the module is inserted into the Catalyst 6500 switch, the WLSM is configured with a VLAN to communicate to the supervisor. Next, the supervisor is configured with a VLAN to communicate to the Catalyst 6500 Series WLSM with one tunnel interface per mobility group. Finally, the access point configuration is updated with the IP address of the Catalyst 6500 Series WLSM and each SSID is updated with a mobility group number.

Benefits of SWAN

Cisco lists several benefits for SWAN. The first of these is easier deployment through assisted site surveys. As discussed in two previous Certification Zone tutorials, How to Implement Wireless Networks and Networking without a Net, the site survey process can be lengthy and error prone. It is difficult to design a placement of access points in the typical building that provides coverage over the entire building while keeping the coverage to the building itself. The assisted site survey feature automates this by determining optimal access point settings including transmit power and channel selection. The WLSE-assisted site survey process includes the following five steps:

1. A floor plan is imported into the site survey tool.
2. Access points are provisionally located by hand on the diagram.
3. Aironet access points are installed in these locations in the building.
4. For the site survey, each access point is set to AP Scan Mode. Each access point operates on the same channel at maximum power. Each access point will detect its neighbors. The system will adjust the transmit power, frequency, and other required parameters to properly cover the building.
5. The settings are fine-tuned in Client Walkabout mode. In this mode, someone walks around the facility with a client device. This device sends continuous measurements to the access points. This data is used to adjust the settings.

Operating costs are reduced because the changes and upgrades can be made en masse from a single point, rather than by having to physically visit each device. This is done by creating a policy template for each similar device.

With autoconfiguration, once a policy template is created using the template wizard that is part of the WLSE, each device on the network can be set to that policy. On boot up, new access points receive the WLSE information via a DHCP server and then download the configuration information. Configuration templates based on device type, subnet located on, and required security parameters can be applied to access points. Once in place, these configurations can be monitored to ensure that the devices conform to policy. A nonconforming device can be fixed from a single point.

Higher availability proactively monitors for performance and faults, such as detecting that an access point has failed. When failure occurs, the system compensates by automatically increasing the power and cell coverage of nearby access points.

Security is improved over that available in normal 802.11-based networks by the addition of the ability to detect, locate, and, to some extent, control rogue access points. Security holes are minimized by the ability to apply a consistent set of security policies to all access points.

Sources of RF interference can be detected so that they may be removed. In addition to detection, the SWAN-enabled components will home in to the area where the interference is coming from.

Levels of SWAN

SWAN can be viewed as having three levels of increasingly finer control over the wireless side of the network and integration of that with the wired network. At the most basic level are Cisco wireless devices and those devices that support the Cisco Wireless Extensions. Next are Cisco access points acting as WDS servers. Finally, there is the full SWAN implementation where the wireless

and wired devices are integrated into a seamless network through the WLSE and a WLSM-equipped 6500 Series switch.

With standalone access points, all of the standard security measures, such as WEP, WPA, and EAP/802.1x, are supported. Client adaptors that support the Cisco Wireless Extensions allow the use of a wide range of EAP types.

Parts of SWAN can also work with just access points. When an access point is deployed in SWAN non-switching mode layer 2, Fast Secure Roaming and local 802.1x authentication are supported. This mode requires the access point to be run as a Cisco WDS server. In non-switching mode, the wireless infrastructure is protected against external attacks, such as rogue access points and non-802.11 interference.

When a Catalyst 6500 is used, the access point is used in SWAN central switching mode. In this mode, the WDS server function is moved to the switch. SWAN switching mode adds centralized management and Fast Secure Roaming.

A key feature of this initiative is the ability to authenticate not just users, but access points as well. Once this is done, the communication between the WDS server and the WDS-enabled access point is secured.

ACS

Any 802.1x authentication server will work with SWAN. Of course, Cisco prefers their Access Control Server (ACS). As with most authentication servers, it can control who uses the wireless network, set the privileges for each user, and record audit and accounting information.

Client Adaptors

Any Wi-Fi certified wireless client device will operate at a basic level in the SWAN-enabled wireless environment. For full support, especially the monitoring and security capabilities, the adaptor must be a Cisco device or one that supports the Cisco extensions. The list of devices that support the Cisco extensions is not extensive. The current listing shows only 51 devices from 15 companies. Dell and Toshiba account for most of these.

Security

Enhanced security is a major part of the SWAN initiative. Proper security for a wireless network is currently a complex and difficult task. The SWAN elements help because they can centralize the management of the security for the wireless network as well as provide a single point of entry control for wireless traffic. However, they do not and cannot sort out the various competing methods that are available for securing a wireless network. This is because the industry has not settled on a single best method for securing wireless networks. To date, this effort has progressed through three generations of approaches to wireless security with additional variants of these. Because this is a vital area, let's briefly look at the state of wireless security methods.

Approach to Wireless Security

There are two aspects to wireless security: authentication and encryption. Authentication seeks to control access to the network. Encryption seeks to hide the transmitted data. 802.11-based wireless networks have procedures to implement each of these security approaches. Unfortunately, both aspects contain holes.

Authentication Methods

Authentication is the weakest -- some would say virtually nonexistent -- part of the 802.11 standards. Three methods are available.

- Open System Authentication relies on the network name or SSID. If the SSID of an access point does not match the SSID of the client, no connection is made.
- The second method, Shared Key Authentication, uses a challenge-response mechanism for authentication. This is a six-step process.
    1. The station sends an authentication request to the access point.
    2. The access point sends a challenge to the station.
    3. The station encrypts the challenge using the active encryption method's pre-shared key.
    4. The station sends this response to the access point.
    5. The access point decrypts the response.

6. If the decryption is successful, the station is authenticated.

Cisco suggests not using shared key authentication due to the security risks. They prefer open system.

- MAC address matching is the last method. The network manager adds each MAC address that should be allowed to authenticate to a list maintained in each access point. MAC addresses are easy to discover and spoof.

There are two problems with these three authentication methods. First, all of them are easily bypassed. Second, they authenticate only a device, not a user.

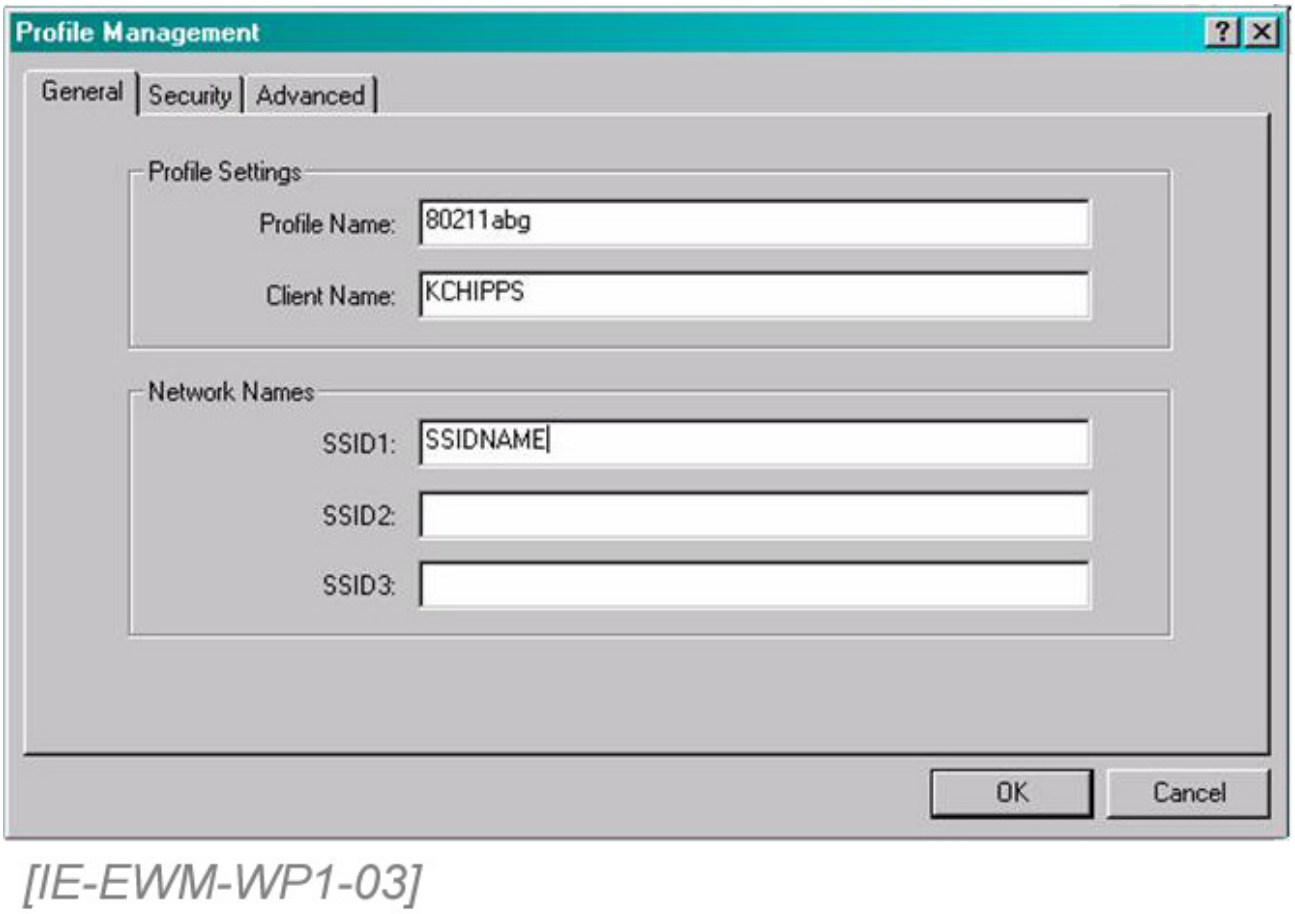
Configuring Authentication in Cisco Devices

All there is to Open System Authentication configuration is the entry of the SSID in each device, For example, this procedure works for a Cisco 1200.

```
interface dot11radio0
ssid ssid-string
```

The *ssid-string* is the network name

For the client adaptor, this is done from a GUI program called the Cisco Aironet Desktop Utility. From the main screen, select the profile to modify. Click on the Modify button. Select the General tab. Enter the SSID in the box.



[IE-EWM-WP1-03]

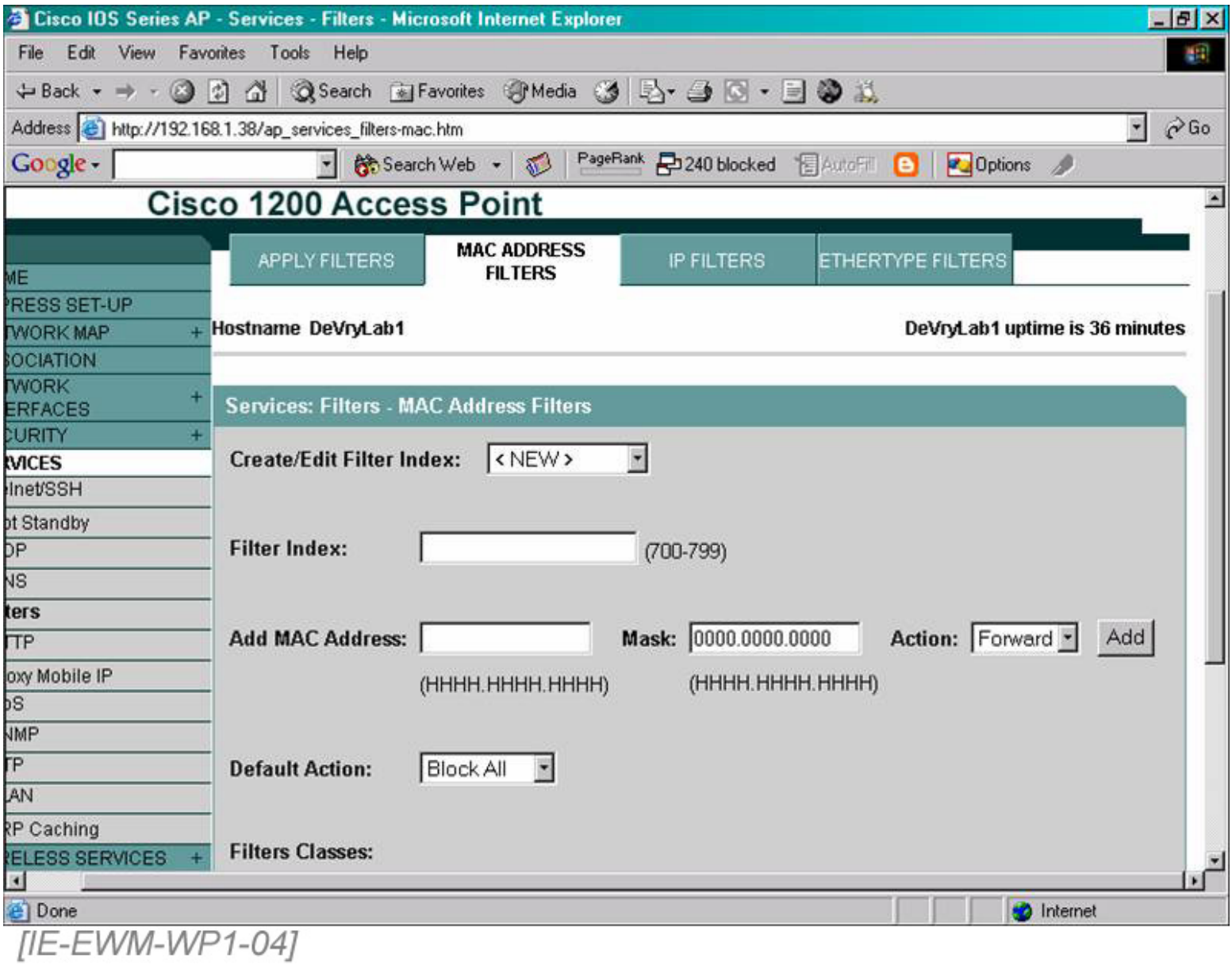
Figure 3. SSID Entry for a Cisco Client Adaptor

Do not use spaces in this name.

Configuration of the shared key as used with WEP is shown below.

The last authentication method is MAC filtering. This must be done from the browser interface. From the main screen, click on the

Services button. From the Services screen, click on the Filters button. Finally, click on the MAC Address Filters tab. The following screen appears:



[IE-EWM-WP1-04]

Figure 4. MAC Address Filtering for a Cisco Aironet 1200 Access Point

Encryption Methods

The main emphasis on security in 802.11 wireless networks has been on encryption not authentication. Encryption has progressed through three generations. These are WEP, WPA, and the WPA2 implementation of the 802.11i standard. The first of these, WEP, has proven to be ineffective except in simple installations. The second, WPA, improves on WEP's encryption. The third and current generation, 802.11i (also called WPA2), solves both the authentication and the encryption problems, but at a high administrative cost. Notice that WEP is used for both authentication and encryption. This is a bad idea because breaking it in a single use compromises both uses. This is why Cisco recommends Open System authentication.

WEP - Static Version

The first generation 802.11 security mechanism is WEP. Wired Equivalency Privacy (WEP) is part of the original 802.11 standard from the IEEE. It is properly maligned for its weakness, but keep in mind what it is for. As the 802.11 specification from 1997 says in clause 8.2.1:

> "Eavesdropping is a familiar problem to users of other types of wireless technology. IEEE 802.11 specifics a wired LAN equivalent data confidentiality algorithm. *Wired equivalent privacy* is defined as protecting authorized users of a wireless LAN from causal eavesdropping. This service is intended to provide functionality for the wireless LAN

equivalent to that provided by the physical security attributes inherent to a wired medium."

There are two key phrases here. The first is in the last sentence. This is the cause of the complaints. Physical security equivalent to a wired LAN is not possible with WEP as will be detailed below. On the other hand, keep in mind that WEP is intended to protect users from casual eavesdropping. As is also detailed below, WEP is adequate protection against causal eavesdropping. Casual eavesdropping does not include loading up a computer with AirSnort or WEPCrack. It does mean your neighbor in the house next door may see your radio signal, but cannot recover the data from that signal. There are over 105 million households and over 6 million business establishments in the United States of America. What is the likelihood that someone will spend from several hours to several weeks to break the passphrase for any particular location? WEP is adequate to protect against causal eavesdropping. But it does not provide the level of protection that a physically secured building provides to a wired network.

The standard calls for securing only the wireless part of the data transmission. The data from the access point to the wired network is unsecured. This is not unusual, as most data carried on wired connections is plaintext. If the physical security of a location is breached, then nothing is safe no matter what is done.

WEP is optional. Most devices, including the latest from Cisco, arrive from the vendor without WEP being enabled. Most users do not know that WEP even exists, much less how to enable it. Due to export restrictions at the time the standard was created, the standard calls for using only 40 bits of encryption. Most vendors also provide higher levels. These higher levels are usually interoperable, but not always.

WEP works like any method that disguises data, by encrypting it. Using an algorithm, the data called plaintext is turned into ciphertext. At the other end, the algorithm is used to reverse the process. Here is the sequence of events as shown in the 802.11 standard.

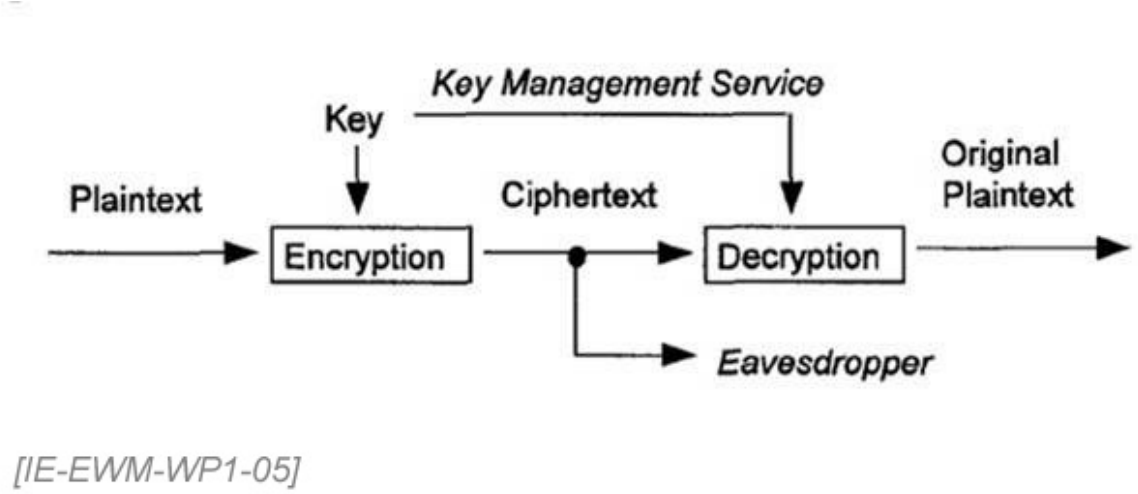


Figure 5. The WEP Process as Illustrated in the IEEE 802.11 Standard

In this case and in most cases, this process is done using four elements. For WEP, the four elements are the data or plaintext being sent, a shared key or password, the encryption algorithm, and a random element. Let's look at each of these elements.

The data is the reason for the network. This is the information sent over the wireless part of the network and what we want to protect from prying eyes. The other three elements are used to protect the data.

The shared key is a password, also called a pass phrase. The form of pass phrase used in WEP is a symmetrical key. That means that the same pass phrase is used at both ends of the conversation. This method requires that the pass phrase be kept secure at both ends. Most implementations use a single key. The standard allows for up to four. These additional keys are used for rotation of the key in use. This is a nice idea, but changing a key still requires manual intervention at each device. The Key ID is a single byte with a value of 0, 1, 2, or 3 corresponding to the active key.

To encrypt and decrypt the data, an encryption algorithm is used. For the WEP implementation, the algorithm is the RC4 cipher. This is a stream cipher. A stream cipher encrypts small chunks of data. The stream cipher is like a conveyor belt. Material is continuously feed in one end, transformed, and moved out the other end byte by byte. The other way to do this is with a block cipher. A block cipher acts on bigger chunks one at a time. RC4 is a product of RSA Security from 1987. RC4 operates by generating a pseudo random sequence of bytes called the key stream. The key stream is combined with the data using an exclusive OR (XOR) operation. The XOR process combines two bytes into one. This is done by comparing each bit of the two bytes to each other. If the two bits are the same value, then the result is a zero. If the two bits are different, then the result is a one. For example:

0	0	1	1	0	1	0	1
XOR Operation							
1	1	1	0	0	0	1	1
Result							
1	1	0	1	0	1	1	0

Using just the pass phrase and an encryption algorithm is not enough to secure the plaintext. An additional element is needed. This element must be random in nature, since the other three elements can be determined. The data being sent can be ascertained by sending your own data or by identifying data that always shows up in a typical transmission. The pass phrase can be guessed through a dictionary attack if it is weak password, discovered through social engineering, acquired by stealing a laptop, or computed. With a known data element and a captured version that was encrypted, comparison of the two will yield the pass phrase without a third element. The third element in WEP is the initialization vector (IV). This is supposed to be random. In WEP, the IV is a 24-bit value. To decode the data, the receiving end must know the pass phrase and the IV value. The pass phrase never changes. The IV changes for each packet. In WEP, the IV is added as plaintext to the encrypted data. At the other end, this known IV is pulled from the transmission and combined with the pass phrase that is stored at the local machine to decode the encrypted data.

To summarize, the process works this way. The algorithm combines the plaintext and the key. Then the random element is added. At the other end, the random element and the key are used to reverse the process. The algorithm in this case takes a block of plaintext and XORs it with a pseudorandom key sequence of equal length. The WEP algorithm using the secret key and the random IV creates this key sequence. In this method, the secret key stays the same, but the random element changes.

To ensure that the data is not changed during transmission, an integrity check vector (ICV) checksum computed using the CRC-32 algorithm is added to the above to complete the transmitted frame. The CRC-32 algorithm is detailed in RFC 3309. The checksum is calculated based on the data in the frame. This method is subject to bit flipping. This is because CRC-32 is linear. An attacker can flip bits in an otherwise encrypted message then correctly adjust the checksum. The arriving message appears to be unchanged.

Part of the resulting frame is encrypted and part is not. As in

Unencrypted		Encrypted	
MAC Header	IV	Data	ICV

For this frame, the IV and Key ID are unencrypted. The data and ICV are encrypted.

At the front of the standard frame are four bytes for the IV and toward the end are four bytes for the ICV. The IV's four bytes include the 24-bit IV, one byte of padding, and the rest for key identification. By implementing WEP, the frame length is increased by eight bytes.

The major implementation problems include the use of static keys, easily known data in the transmission, and a limited size IV. Of these, the first and last are the major problem areas.

The secret static key was expected to be the only weak point. Even this was not seen as a major weakness. As the IEEE says:

> "The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack. This in turn is related to the length of the secret key and the frequency of the changing key. WEP allows for the changing of the key (k) and frequent changing of the IV."

A key may be ascertained or stolen. Most implementations select a key when the wireless devices are first deployed. After that, the key is rarely if ever changed. This is due to a lack of centralized management for wireless devices. To change a key, the network administrator must touch each device. Few will do so on a regular basis. Many keys are simple, short, ASCII words turned into hexadecimal by the system.

There is also known data in most transmissions. As Stubblefield, Ioannidis, and Rubin point out:

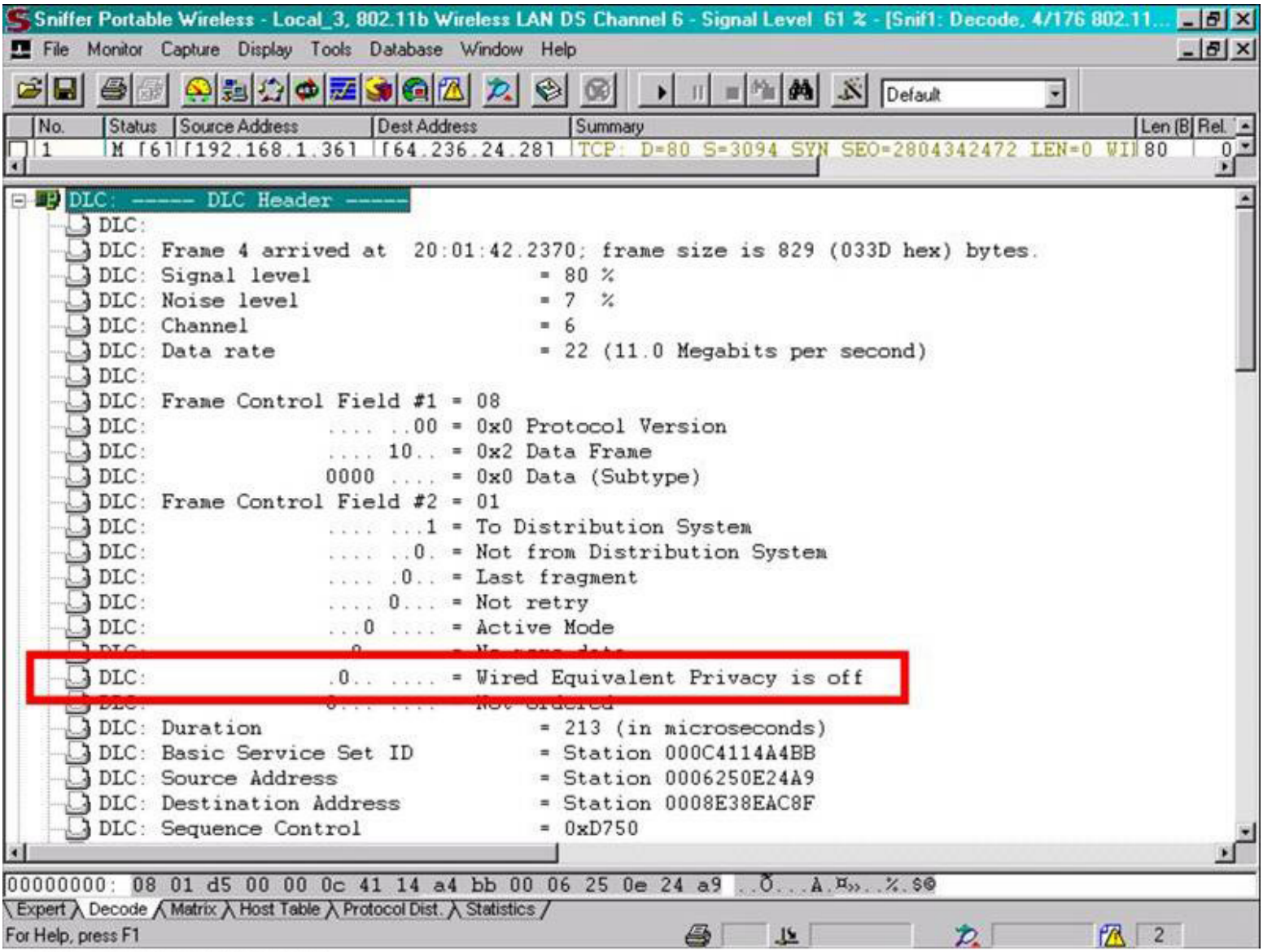
> "This discovery actually made the attack even easier, as all the IP and ARP packets would now have the same first plaintext byte (oxAA, the SNAP designation)."

The main problem with the WEP implementation is the high likelihood that the IV will be discovered. This method is the one most commonly used to break into a WEP protected system. Since the IV is a 3-byte value, there are only 16,777,216 possibilities for

the IV. As any IV is random, rather than sequential, it is likely that an IV value could be repeated after as few as 5,000 transmissions. The transfer of a single large file can produce this number of transmissions.

Let's summarize the problems. First, by allowing the keys to be manually entered, which they typically are, they are never changed in practice. Second, the IV space is too small. Repeats happen too quickly, which allows the IV to be cracked. Third, a short pass phrase is a problem, but this is less important than the weak IV. This is because lengthening the pass phrase does not overcome the IV's weakness. Lastly, WEP is not even required.

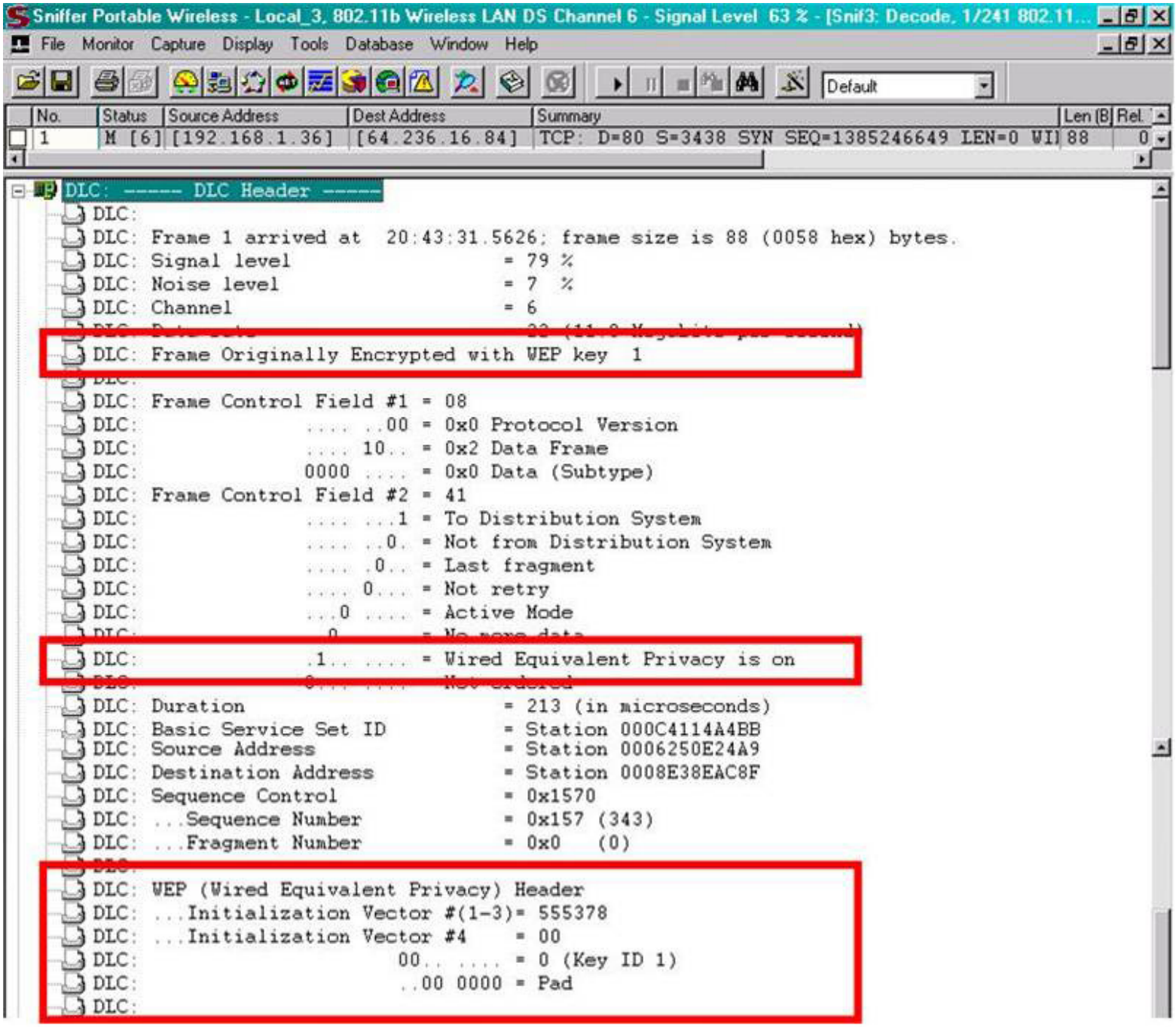
What does WEP look like in practice? An unprotected frame looks like this:



[IE-EWM-WP1-06]

Figure 6. An Unprotected 802.11b Frame

A frame using WEP looks like this:



[IE-EWM-WP1-07]

Figure 7. A WEP-Protected 802.11b Frame

The easiest way to break into a system that uses WEP for encryption is to discover the IV. Then this value can be used to reveal the secret key. To do this, a program such as a wireless network analyzer or sniffer is used to collect enough data for a program like AirSnort or WEPCrack to discover the IV.

Configuration of Static WEP

On a Cisco 1200 access point, WEP configuration is simple. The steps are done in global configuration mode.

To enable WEP for the 2.4 GHz radio

```
interface dot11radio0
encryption key 1 size 128 thepassphrase
```

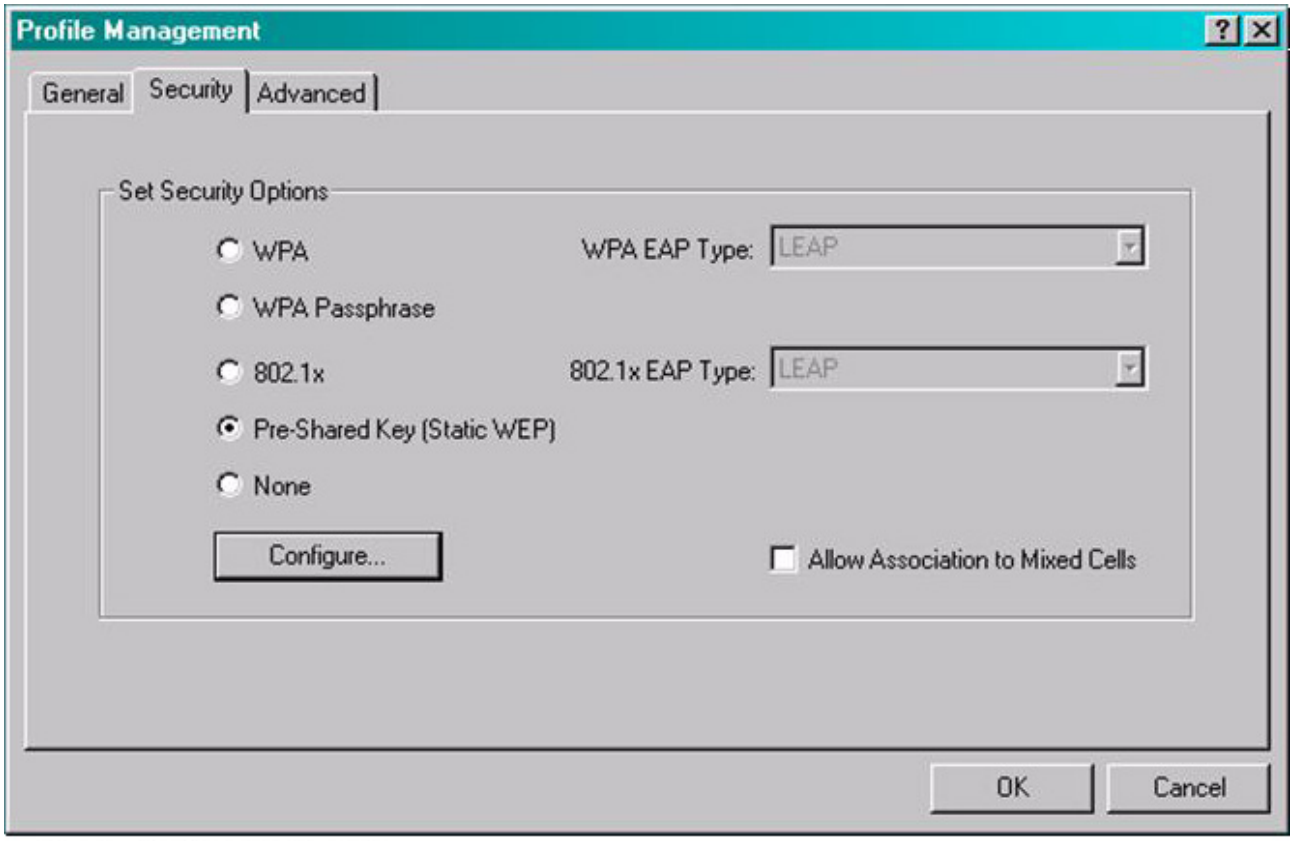
For the 5 GHz radio

```
interface dot11radio1
encryption key 1 size 128 thepassphrase
```

In this case, the term *thepassphrase* is the hexadecimal password. Since the maximum number of bits should be used, this should be 26 hexadecimal digits.

As discussed above, the **key** subcommand is how the four different keys are specified. Any of the four possible keys can be used.

At the other end, the Cisco AIR-CB21AG Cardbus client radio is configured from a GUI interface. This program is called the Aironet Desktop Utility. From the opening display, the Security tab is selected. This produces the following screen:



[IE-EWM-WP1-08]

Figure 8. Selection of Static WEP on a Cisco Client Adaptor

From this screen the Pre-Shared Key (Static WEP) radio button is selected. This selection produces:

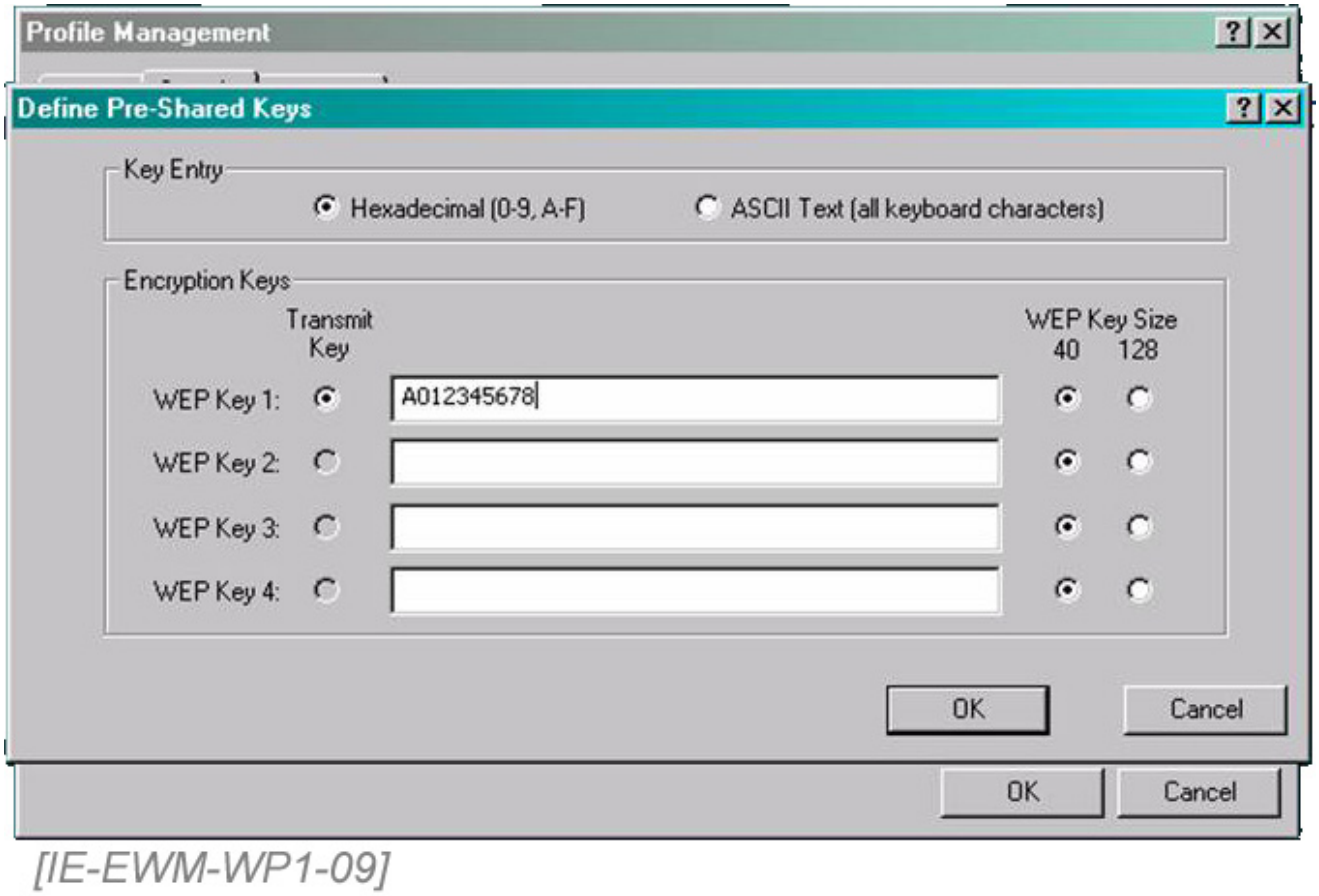


Figure 9. Entry of the passphrase for Static WEP on a Cisco Client Adaptor

Here, the hexadecimal pass phrase is entered. In this case, the key or pass phrase is A012345678, which is too short.

WEP - Dynamic

A variant of WEP is called Dynamic WEP. It uses some form of EAP to provide a different WEP key for each user. Since they change frequently, dynamic WEP keys prevent the discovery of the key. In addition to changing the key, it can be hashed using Temporal Key Integrity Protocol (TKIP). EAP acts only on unicast frames. To provide protection to broadcast and multicast frames, broadcast key rotation must be enabled.

Configuration of Dynamic WEP

Only a few additional commands are required to enable dynamic WEP.

```
configure terminal
interface dot11radio 0
encryption key 1 size 40 cisco
encryption mode wep mandatory mic key-hash
broadcast-key change 300
```

`mode wep` enables WEP. To enforce the use of WEP, add the mandatory keyword. If this is omitted, the access point will talk to both WEP and non WEP-enabled clients. The Message Integrity Check is enabled with **`mic`**. To hash the key **`key-hash`** is used. Key rotation for the broadcasts is enabled with **`broadcast-key change 300`**. In this case, the number of seconds is 300. It can be any value from 10 to 10000000. Cisco states that if you enable broadcast key rotation on one radio in a dual radio access point, it is enabled for both radios.

WPA

Wi-Fi Protected Access (WPA) is an improvement over WEP. It provides a stronger message integrity check via MIC, a per-packet keying function, and replay protection. There are two versions of WPA. WPA-Personal protects unauthorized network access by utilizing a static password just like WEP. WPA-Enterprise verifies network users through a RADIUS server.

Using WPA is not a straight path. For older equipment, the firmware must be upgraded. Newer equipment comes with this support built in. For example, support for WPA in the 1100 and 1200 series access points was announced in Product Bulletin 2179 dated 3 October 2003. Products produced after that date are ready to go. The product bulletin discusses what needs to be done to the older models. WPA requires that the access point run the IOS. VxWorks does not support WPA.

In many cases, one aspect of a wireless system is not compatible with another. For example, one of the main Cisco enhancements to support mobility in wireless devices, Fast Secure Roaming, is not entirely compatible with WPA. As Cisco says:

> "While the key generation mechanism used with fast secure roaming is not a current component of WPA or the IEEE 802.11i specifications, Cisco has submitted this mechanism to IEEE 802.11i for future inclusion. Additionally, Cisco compatible clients that comply with Version 2 of the Cisco compatible specification will support fast secure roaming."

What exactly is WPA? How does it improve on WEP? WPA improves both authentication and encryption. Authentication is improved by the acknowledgment of the commonly used 802.1x and EAP for authentication. Encryption is improved by the use of the Temporal Key Integrity Protocol (TKIP) and an enhanced integrity check method called MIC.

To implement WPA, an authentication server, such as a RADIUS server, is set up. This provides authentication both of the user and the access point. With a RADIUS server, the access point knows whom it is talking to since the user must login. The users also know that they are talking to an authorized access point because they are the only ones who can talk to the authentication server. All of this is done using a combination of 802.1x and one of the EAP types.

802.1x is a port-based authentication, not encryption, method. When using 802.1x, the user who desires access to the network through an access point is called a supplicant. The access point is an authenticator. The RADIUS server is the authentication server. Using these three devices, the user asks for access. The access point passes the request to the authentication server. Based on the credential submitted by the user, the authenticator is told to accept or reject the supplicant. RADIUS handles only the traffic between the authenticator and the authentication server. RADIUS is a straightforward set of requirements detailed in several RFCs.

EAP is used to protect the traffic between the authenticator and the supplicant. EAP itself is designed to carry arbitrary authentication information. It typically rides on top of another protocol, such as 802.1x or RADIUS. EAP is discussed in RFC 2284. 802.1x is used to carry the authentication information in the form of EAP payloads. The combination looks like this.

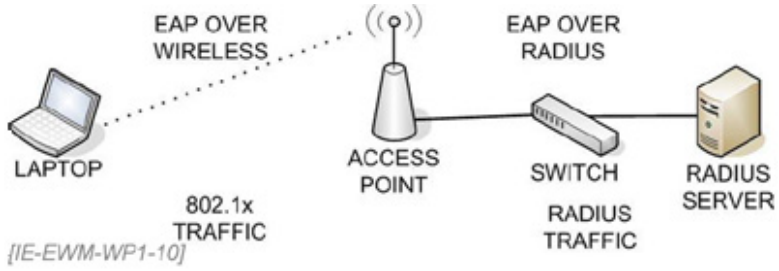


Figure 10. Use of EAP for Data Protection

Unfortunately, there are many forms of EAP. EAP itself, as defined in RFC 2284, is used to transport authentication information. It seems like there are new EAP methods every month. Neither the standards nor the industry agrees on the best choice. Let's look at an example of the type of problem this causes. Here is part of an email message exchange on this very subject.

```
We were able to get Cisco PEAP to work with Novell and the ACS server,
but only with Cisco wireless cards. The customer doesn't actually have
Cisco cards they are using laptops with builtin Intel cards and we
weren't successful in getting them to work even though they support
Cisco PEAP. This could just be a configuration error, but it looks
like they couldn't get past phase 1 of the negotiation with the ACS
server. Cisco cards worked fine using Cisco PEAP and setting the ACS
server to talk to the Novell NDS database using generic LDAP.

We also tried EAP-FAST and that did not work either. The error on the
ACS server said that the external database did not support the
authentication type, same error we got using LEAP or MS-PEAP. Have you
actually configured EAP-FAST in your environment to work or are you
going on what Cisco has told you? If EAP-FAST is supposed to work,
does it only work with Cisco wireless cards or is it supposed to work
with non-Cisco cards as well, with or without the Cisco compatible
extensions supported? We were trying the EAP-FAST protocol on the
```

Intel cards, although we didn't try it on the Cisco cards for testing.

Options include EAP-MD5, EAP-FAST, EAP-TLS, EAP-TTLS, LEAP, EAP-SIM, and PEAP. The current trend is toward PEAP.

EAP-MD5 is always mentioned, but rarely used. EAP-MD5 was once popular, but no longer. It is vulnerable to dictionary and brute force attacks. For the client, MD5 uses an MD5 hash of the username and password. It uses static WEP keys, so it provides nothing in addition to standard WEP. There is no mechanism for the access point to be authenticated.

EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling) was developed by Cisco. This EAP type was developed for customers who cannot enforce a secure password policy or deploy a certificate server. EAP-FAST does its work through a tunneled authentication process using symmetric key algorithms. An AAA server is required to provide the client with someone to talk to in order to establish the secure tunnel after each side has been authenticated. Once the tunnel has been established, the client's username and password are sent over this secure connection.

EAP-TLS is secure, but difficult to use, because it requires digital certificates for both client and server. This requires that the certificates be purchased from an outside source or be created by an in-house server. TLS stands for Transport Layer Security. RFC 2716 defines EAP-TLS.

EAP-TTLS is Tunneled Transport Layer Security. This is a combination of certificates and passwords. The access point authenticates to the client using a certificate. The client authenticates with a username and password sent over an encrypted tunnel.

LEAP - Lightweight EAP was Cisco's favorite until a hole was found in it. It is password based. LEAP uses MS-CHAPv1, which is unencrypted, for authentication. MS-CHAPv1 can be broken by use of an offline dictionary attack. A good password policy will prevent this. Of course, few users will actually use a 12- to 16-character string of random numbers and letters.

EAP-SIM is EAP-Subscriber Identity Module. These are SIM cards such as are found in cell phones. This is a new method being discussed, but not yet widely used.

EAP-PEAP is a hybrid of certificates and passwords. PEAP means Protected Extensible Authentication Protocol. PEAP is popular because it adds capability required in a wireless network to the basic EAP-TLS mechanism, while avoiding the problem of client certificates. Only a server side certificate is required. The PEAP portion of the conversation is between the supplicant and the server. The access point merely passes the traffic back and forth. An additional advantage is that updates can take place by changing only the client and server.

TKIP addresses the weak encryption used in WEP. TKIP improves on WEP by using a 256-bit encryption key. By combining the client MAC address, a 48-bit IV, and a 128-bit temporary key, TKIP produces this longer key. The key is called temporary because it is changed every 10,000 frames. To provide further integrity to the transaction, the ICV is replaced with a 48-bit IV instead of WEP's 24-bit IV. TKIP uses a hierarchy and key management method that removes the predictability that provided a door into WEP. However, to do this key management, an authentication server is required. Using the 802.1x specification, the server provides a unique key for each session between a workstation and an access point. TKIP provides better protection for the wireless data through a per-packet key, a better message integrity check, and a larger IV. TKIP uses the master key to create new keys, which are changed on a regular basis. No key is reused.

The last part of this new process is the Message Integrity Check (MIC). The MIC part prevents a hacker from capturing data frames, altering them, and resending them. MIC avoids the bit-flipping problem seen in CRC-32.

There are two versions of WPA. The main version is WPA for the Enterprise. This version includes both authentication and encryption. WPA for the Home has only encryption.

WPA for the Enterprise

In addition to the basic WPA setup for the Enterprise version, a RADIUS or similar service is required. For this to work, the RADIUS must exist, the access point must support WPA, and the clients must as well.

WPA for the Home

WPA for the Home is a subset of WPA for the Enterprise. The main change is once again a lack of authentication. Just like WEP, WPA for the Home uses a shared key that must be entered by hand into each device's configuration.

Wireless Security Suite

Cisco calls their implementation of WPA the Cisco Wireless Security Suite. It operates with Aironet access points and Cisco Compatible Extensions client devices. This is not part of SWAN, but it supports and is supported by SWAN.

Configuration of WPA

To enable WPA on an access point that supports it from the command line, enter the following for each radio.

```
encryption mode ciphers tkip
```

This line specifies the cipher method. In this case, TKIP.

```
authentication open eap eap_methods
```

Sets up an EAP method for non-Cisco clients.

```
authentication open network-eap eap_methods
```

Sets up an EAP method for Cisco clients.

```
authentication key-management wpa
```

Activates WPA.

This configuration can also be done from the web interface's Security-Encryption Manager and SSID Manager pages.

Breaking into WPA

Of course, as soon as WPA became widely deployed someone found a hole in it. This hole is not very large and not unexpected. The problem is the use of short pass phrases in WPA for the Home. In this pre-shared key version of WPA, when a short pass phrase (less than 20 characters) is used, a dictionary attack could discover the key. Even worse, data can be collected on site and the dictionary attack can then be run off site over time.

To solve these problems, just use a long, random pass phrase. Just like today when using WEP, few will do this. Long means more than 20 characters. "Random" means a string of characters that is unlikely to be discoverable through a dictionary attack.

WPA2

As first seen in WPA, security in wireless networks is moving from mere encryption to true authentication. This movement is seen in the Enterprise version of WPA at a basic level. In WPA2 (802.11i), it is seen fully developed.

Wi-Fi Protected Access 2 (WPA2) improves on WPA by adopting the 802.11i standard. When WPA was approved, 802.11i was not finished. However, many aspects of 802.11i were known. The main difference over WPA is the use of AES-CCMP or Advanced Encryption Standard - Counter Mode/CBC-MAC Protocol. This is a block cipher. AES is a National Institute of Standards and Technology (NIST) FIPS 140-2 compliant encryption algorithm. Just like WPA, WPA2 can be enabled in two versions. 802.11i protects the data and selected header fields.

The process works in the following manner. When a client requests access, an 802.11i-enabled access point responds with a Robust Secure Network (RSN) Information Element. This advises the client of the access point's available authentication and cipher methods. The client selects one it can use and begins an open system authentication connection to the access point. The access point verifies the credentials and completes the association. Next, 802.1x-based authentication starts. The user must authenticate to the RADIUS server. The authentication server creates a pairwise master key (PMK). This key is sent to the access point. The access point sends it on to the client. This key controls the client's access through the wireless media. From this is derived the Pairwise Transit Key (PTK). This is a set of keys that mutually identify the device and secures the data. Each PTK is specific to the client access point conversation. This requires reauthentication upon roaming.

Most hardware will need to be of recent origin, developed with 802.11i in mind. This is due to the higher computational load that this method places on the equipment. This is not just a firmware upgrade for most brands. For Cisco, the 1130 AG and 1230 AG support WPA2 out of the box. The 1100, 1200, and 1300 series require an IOS upgrade. 802.11b-only Cisco devices cannot support WPA2. Devices that support the Cisco Compatible Extension Version 3 will handle WPA2 as well.

Summary of the Three Security Generations

	WEP	**WPA**	**WPA2**
Encryption Algorithm	RC4	RC4	AES

Key Management	None	EAP	EAP
Key Length	40 bits	128 bits	128 bits
Data Integrity	CRC-32	MIC	CCM
Header Integrity	None	MIC	CCM

Additions to the Basic Security Methods

Additions are often made to the three basic methods in order to harden them further. These additions include:

- MAC Address Filtering
- One MAC per port
- VLAN
- VPN

MAC Address Filtering

MAC address filtering is a simple addition to wireless network security. It works by the administrator making a list of all of the MAC addresses of the client radios authorized to access the wireless network as discussed above.

Set MAC Address per Port

If each switch port has a single MAC address that is allowed through, then no one can plug a rogue access point into the wired network without first altering the access point's MAC address.

The configuration is:

```
switchport port-security maximum 00-aa-bb-d1-01-56
```

VLAN

With the number of security risks imposed by adding wireless devices to a network, many administrators have chosen to isolate and control the wireless portion of their networks. This is commonly done by using a VLAN. In this configuration, all of the access points are connected to switch ports that are assigned to a particular VLAN. This allows access back into the wired portion of the network to be controlled by an access list or firewall.

VPN

A VPN is used to add additional encryption on top of or instead of that provided by WEP. As seen above, WEP is easily cracked. VPNs came into use to provide a better method of data encryption. The VPN can be set up through an existing router, firewall, or VPN concentrator.

Management Security

Regardless of the security method, some basic changes should be made to any access point to better secure it. These management-related changes include altering the default SSID, username, and password for the access point. For Cisco devices these are:

- SSID - tsunami
- Username - Cisco
- Password - Cisco

Unless you are advertising for clients, the SSID should not provide anything that would identify the organization, where the device is located, or the type of access point it is.

Turned on by default, which should be turned off are:

- Telnet
- CDP
- http

Management of devices via Telnet or http is a common practice. SSH is a better alternative, as it is inherently secure.

Turn off Cisco Discovery Protocol. This is not useful for a wireless device because it allows an outside wireless device to go the other way to locate an authorized access point.

All unneeded services, such as http access, should be disabled. This will limit the avenues of attack to the access point.

SNMP access is always a security hole. Versions 1 and 2 of SNMP have no security to speak of. The Cisco access points only support SNMPv1 and v2c. When SNMP is used, the default password, public, needs to be changed. Access should be read only, never write. Cisco access points arrive with SNMP turned off.

Use a separate subnet for wireless traffic. This helps to isolate and identify wireless-related traffic.

Set the number of MAC addresses per port to one. This will help prevent rouge access points since any access point attached to that port and any clients that attach through the access point would have different MAC addresses. The basic command for this is:

```
switchport port-security maximum 1
```

The range is 1 to 128. The default is 128. This command sets it to one MAC address. An additional action command can be used to shutdown the port. This is:

```
switchport port-security violation shutdown
```

In this case, the **shutdown** command places the port into the error-disabled state. Then it sends an SNMP trap notification. The **protect** option drops the packets with unknown source addresses until the number of MAC addresses falls below the value set. With the value set to 1, this subcommand and the **restrict** subcommand, which is similar, are not needed.

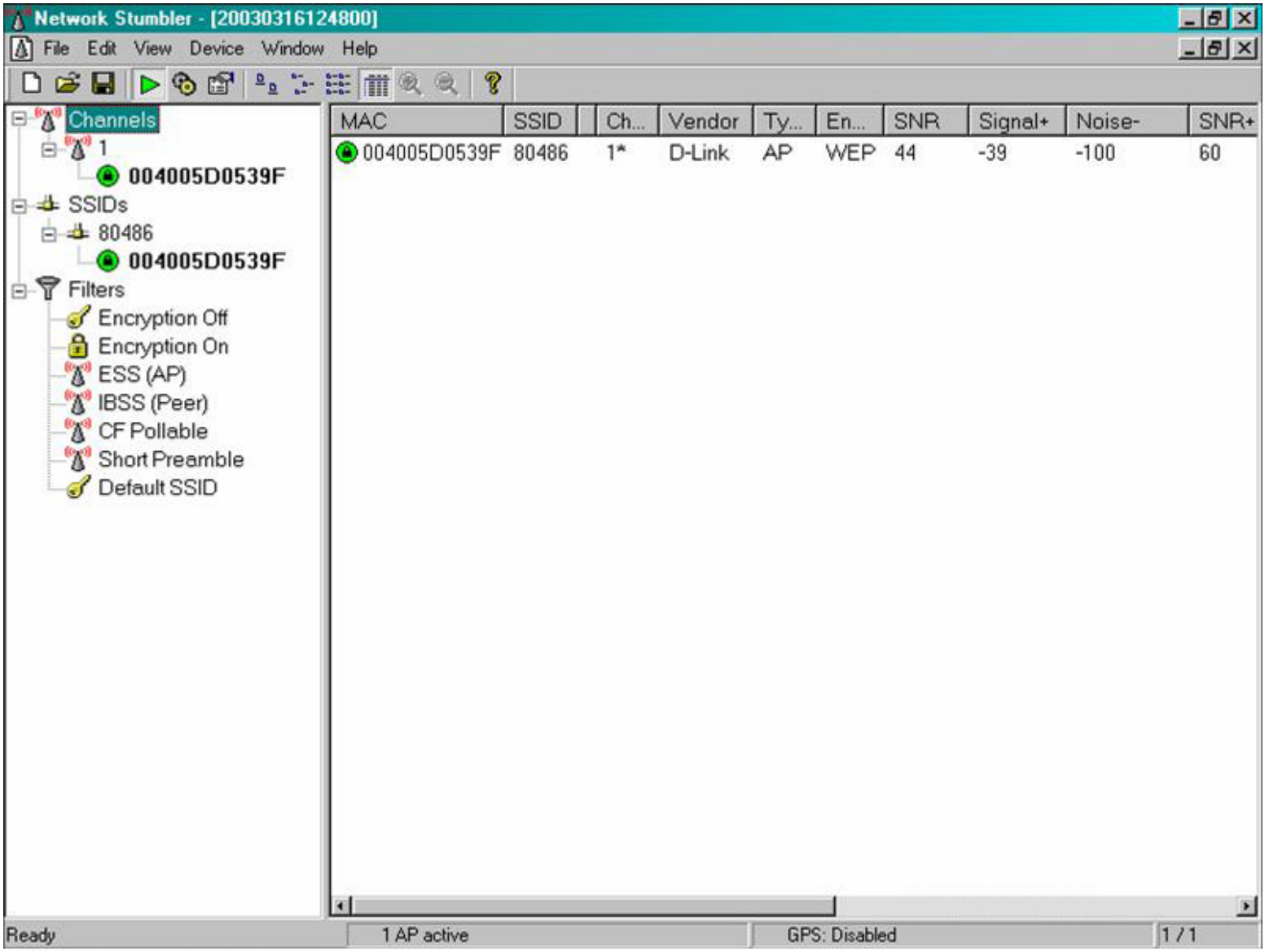
Hacking Techniques

Attacks on wireless networks can take many forms. Common methods include sniffing packets, surveillance, wardriving, RF jamming, and rogue access points. Of these, only rogue AP detection is currently handled by SWAN.

Rogue APs

Rogue access points are those not installed by the IT department. They may have been installed by a user or by someone attempting to break into the network.

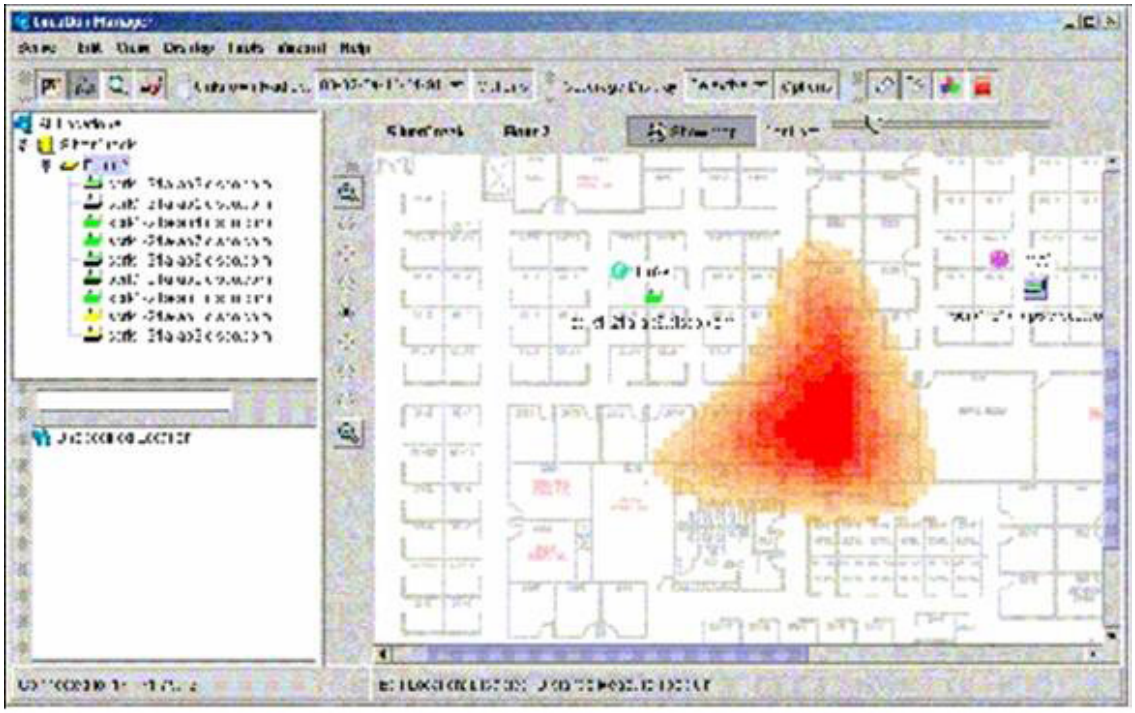
Detection of rouge access points may be done wirelessly or from the wired side. From the wireless side, the easy ones are found by walking around with a laptop running Windows XP or a program like NetStumbler. This produces a display such as this:



[IE-EWM-WP1-11]

Figure 11. NetStumbler Screen

This works well for innocent rogue APs. A more sophisticated method is deployed by Cisco as part of the WLSE card. This method uses both the authorized access points and the client wireless NICs that support the Cisco extensions to locate and disable rogue access points. These both report when not transmitting or receiving. The access points and enabled clients when not transmitting or receiving jump to an adjacent channel to look for foreign signals. The information collected is sent to the WDS server. The WDS compiles the data and sends it on to the WLSE. The Location Manager function in the WLSE will use the received data to triangulate the location of the rogue device. This same data allows the general location of client devices to be fixed as well. When an unauthorized access point is identified, it is displayed on a map of the site. The actual device must still be located.



[IE-EWM-WP1-12]

Figure 12. Rogue Access Point Location Indicated by the Orange Area

From the wired side, most innocent APs can be detected by scanning for open port 80 on a device. Because the user side of the network should not normally have any web servers running, this will detect APs that are administered via a built-in web browser. Most consumer grade access points that the typical user would buy and install are administered in this manner.

Many local area networks do not have any installed access points. The network administrators are very careful about discovering any access points that are installed by employees or hackers. They never consider the opposite problem. In addition to access points, many computers are coming equipped with 802.11 capable radios installed as standard equipment. To be "helpful", some of these are turned on by default. Most of these come with Windows XP installed. To be helpful, Windows XP immediately goes looking for wireless networks. By doing so, the hacker need only turn on an access point in the vicinity. The helpful laptop with the helpful operating system connects to the outside access point. This same thing can be done without an access point at all. In ad hoc mode, the laptop will connect to any other laptop or other device.

Hardware and Products

It is difficult to see how hardware differs from products. It could be argued that products include hardware and software. This section will focus on the current hardware offered by Cisco for wireless networks. There are three categories: access points, bridges, and client adaptors.

Access Points

WLSE supports Cisco Aironet 1230 AG, 1200, 1130 AG, 1100, and 350 series access points. It also supports the Cisco Aironet 1300 access point/bridge. Cisco 1300 and 1400 series bridges can be configured, monitored, and used to report management data to the WLSE.

Any access point used in a SWAN-enabled system must run the Cisco IOS software. VxWorks is not supported. However, WLSE can manage a mass upgrade of access points from VxWorks to the Cisco IOS.

The original access point offered by Cisco is the 350 series. This is an 802.11b-only product. It has been assigned to end of life status.

[IE-EWM-WP1-13]

Figure 13.

The new line of access points begins with the 1100 series. The Cisco Aironet 1100 Series is a single-band unit. Cisco calls these legacy devices because they support only 2.4 GHz radios. The older 802.11b radios can be upgraded to 802.11g. The units currently being shipped come with an 802.1b/g radio. These units do not have a console port. The antennas are fixed.

[IE-EWM-WP1-14]

Figure 14.

The 1130 AG is a dual radio unit. The 1130 is an indoor-only unit in a plastic case designed for wall mounting. It uses a fixed omnidirectional antenna

Figure 15.

The 1230 AG is a dual radio indoor or outdoor unit. The 1230's antennas can be changed using the dual antenna ports. It is plenum rated.

Figure 16.

Next in line is the 1200 series. This unit can hold two radios. Currently, that is one 2.4 GHz and one 5 GHz radio. When a 5 GHz radio is installed, the antenna is a fixed patch style. The 2.4 GHz radio's antennas can be changed. This was due to FCC restrictions on antenna usage in the UNII-1 band. These restrictions have been lifted, but a revised radio is required to conform to the new regulations. These units can be managed from the CLI using the Cisco IOS or from a web interface. The 1200 can support up to 16 VLANs per radio.

The final access point unit is a combination outdoor access and bridge named the 1300. Cisco states that this unit is suitable for outdoor CAN and MAN deployments. This is a 2.4 GHz-only unit.

Figure 17.

Bridges

The 350 line includes two devices called bridges. One is a wireless bridge as the term is commonly used. The Cisco Aironet 350 Series Wireless Bridge is designed to connect two buildings. It is designed for outdoor use. The other bridge unit is a workgroup bridge. This device connects up to eight wired devices to a wireless LAN.

The new line of bridges begins with the 1400 series. The 1400 uses a UNII-3 5.8 GHz radio. Data rates up to 54 Mbps are supported, depending on distance. The 1400's case is designed for outdoor mounting. Even the power injector can be mounted in harsh, but weather protected, environments. One model has a fixed antenna. The other model comes with an N type connector port.

Figure 18.

Client Devices

Cisco offers five client devices.

- Aironet 802.11a/b/g CardBus adaptor
- Aironet 802.11a/b/g PCI adaptor
- Aironet 350 802.11b PC Card adaptor
- Aironet 350 80211b PCI adaptor
- Aironet CB20A 802.11a CardBus adaptor

Of these, the 350 and CB20A models are older, single band units. The new series supports 802.11a/b/g.

Standards

At the top of the Enterprise Wireless Mobility list are IEEE Standards. This is at the top because everything must flow from these standards. In addition to the IEEE standards, there are other sources of regulations and standards that apply to wireless systems.

Sources of Standards

Standards related to wireless networks come from three main sources. These sources include the regulatory bodies with jurisdiction for the area, the technical standards bodies, and the industry associations with an interest in wireless data networks.

This first section will explain what bodies produce regulations and standards for wireless systems. Then the specific requirements will be detailed.

Regulatory Environment

The regulatory environment for a jurisdiction has a major impact on what can and cannot be done to change a radio frequency system. To illustrate this impact, the regulations that apply in the United States of America (US) will be used. The Federal Communications Commission (FCC) is the main regulatory body for radio frequency systems in the US.

In the US, the main regulatory requirements are contained in the Code of Federal Regulations. As stated at the US government

web site:

> "The Code of Federal Regulations (CFR) is the codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the Federal Government. It is divided into 50 titles that represent broad areas subject to Federal regulation. Each volume of the CFR is updated once each calendar year and is issued on a quarterly basis.
>
> - Titles 1-16 are updated as of January 1st
> - Titles 17-27 are updated as of April 1st
> - Titles 28-41 are updated as of July 1st
> - Titles 42-50 are updated as of October 1st
>
> Each title is divided into chapters, which usually bear the name of the issuing agency. Each chapter is further subdivided into parts that cover specific regulatory areas. Large parts may be subdivided into subparts. All parts are organized in sections, and most citations in the CFR are provided at the section level."

Of interest here is Title 47 - Telecommunication, Chapter I - Federal Communications Commission, Part 15 - Radio Frequency Devices. These are the regulations that govern devices using unlicensed frequencies. Part 101 covers devices using licensed radios for the most part. Other jurisdictions have similar regulatory structures.

IEEE

The second set of requirements comprises those that arise from the standards creation bodies. The IEEE is the most active organization in the wireless standards process.

Wi-Fi Alliance

The Wi-Fi Alliance, an industry group, has taken the original specifications from the IEEE and organized them into product certification packages.

Radio System Related Standards

The IEEE has also defined the set of standards that dictate how a wireless radio system should be constructed. Let's look at the 802.11 set of standards.

As of the date of this publication, the IEEE 802.11 standards that define a complete wireless communication system are:

802.11 approved in July 1997

802.11a approved in September 1999

802.11b also approved in September 1999

802.11g approved in June 2003

A supplemental security standard is:

802.11i

Supplemental standards approved that are of interest mostly to the manufacturers of the equipment include:

802.11c

802.11d

802.11f

802.11h

Supplemental standards that supplement those listed above are:

802.11e

802.11n

802.11j

802.11k

802.11p

802.11r

802.11s

802.11t

802.11u

802.11v

Other 802.11 groups:

802.11m is a proposed maintenance group

802.11l is not assigned at this time.

Let's look at each of these in more detail.

802.11

802.11 is the original wireless standard. It specifies a 2.4 GHz radio. 802.11 is not widely used anymore due to the low data rate of 2 Mbps. Some use is still seen in industrial environments using FHSS.

802.11a

The 802.11a standard specifies 5 GHz range radios at 54 Mbps. 802.11a is meant to be a high speed alternative to 802.11b, operating in the less congested 5 GHz frequency range. The 5 GHz frequency is an advantage in that it is less congested, but in the typical office environment, the range of this frequency is limited.

802.11b

802.11b is the most widely used standard for wireless local area networks. It sees some use in campus area networks as a way to bridge between locations, and as a way to connect to the local area network from anywhere on the campus. 802.11b is currently used to deliver Internet access in metropolitan area networks. It is not well suited for campus and metropolitan area network uses. This is likely a temporary solution, pending 802.16 deployment.

802.11c

802.11c defines procedures required to ensure proper bridge operation. Product developers use this standard when developing access points.

802.11d

802.11d is primarily of interest to equipment manufacturers. It is a supplement to the 802.11 standards. It provides a method for equipment manufacturers to produce equipment that can adapt to the country in which it will operate. This is required because the 802.11 standards cannot legally operate in some countries due to those country's restrictions on the use of the frequencies. 802.11d defines additions and restrictions to the basic 802.11 standards to allow them to do so. As the abstract to this standard says:

> "This amendment specifies the extensions to IEEE Std 802.11 for Wireless Local Area Networks providing specifications for conformant operation beyond the original six regulatory domains of that standard. These extensions provide a mechanism for an IEEE Std 802.11 access point to deliver the required radio transmitter parameters to an IEEE Std 802.11 mobile station, which allows that station to configure its radio to operate within the applicable regulations of a geographic or political subdivision. This mechanism is applicable to all IEEE Std 802.11 PHY types. A secondary benefit of the mechanism described in this amendment is the ability for an IEEE Std 802.11 mobile station to roam between regulatory domains."

The impetus behind 802.11d is to promote the use of 802.11 in countries where the physical layer radio requirements are different from those in North America. Equipment manufacturers do not want to have to produce different equipment for each country.

802.11e

802.11e is a yet-to-be-approved supplement to the MAC layer of 802.11 to provide QoS (Quality of Service) for LANs and perhaps increase throughput to up to 35 Mbps. It applies to 802.11a, b, and g. It is uncertain how all of this will work. What follows are some of the indications. First is an addition to the DCF network access method that has been proposed as a way to add QoS by establishing eight traffic categories or priority levels. Using differing interframe spaces, with the highest priority having the shortest space, will create these categories. This does not guarantee service; it just moves some frames to the front of the line. Of course, being on a wireless network, the line may or may not move. Another possibility is the control of data streams to prevent an additional media stream from beginning playback if its traffic will overload the network segment and degrade existing streams. 802.11e also addresses issues of low signal strength and its effect on data throughput. A low signal can result in resends, which reduces overall available bandwidth. Until 802.11e is approved, all versions of 802.11 will have QoS issues that make them less than useful for applications such as streaming video and audio.

802.11f

Primarily of interest to equipment manufacturers, 802.11f is a recommended practice document that provides a means to achieve interoperability among access points from different vendors. This technology, the Inter-Access Point Protocol, handles the registration of access points within a network and the exchange of information when a user is roaming among coverage areas supported by different manufacturers' access points. 802.11f facilitates the hand-off between access points.

802.11g

Approved on 12 June 2003, 802.11g is for the 2.4 GHz band. It is designed to be a higher bandwidth -- 54 Mbps -- successor to the popular 802.11b standard. 802.11g uses the same OFDM modulation as 802.11a but, for backward compatibility, it also supports Barker Code and CCK modulation to support b clients. As an option, PBCC modulation can be included to support 22 and 33 Mbps.

802.11h

The 802.11h standard is a supplement to the MAC layer in order to comply with European regulations for 5 GHz wireless LANs. European radio regulations for the 5 GHz band require products to have transmission power control and dynamic frequency selection. Transmission Power Control (TPC) limits the transmitted power to the minimum needed to reach the furthest user. Dynamic Frequency Selection (DFS) selects the radio channel at the access point to minimize interference with other systems, such as radar. In Europe there is a strong potential for 802.11a interfering with radar and satellite communications, which have primary use designations. Most countries authorize wireless local area networks for secondary use only.

802.11i

This is the revised security standard discussed earlier in this tutorial. The Wi-Fi Alliance calls this WPA2.

802.11j

802.11j is a specification for adjusting the basic 802.11 standards to facilitate their use in Japan. It is mostly of interest to equipment makers. Notice the Japan-related standard is j. Isn't the IEEE just full of funny engineers?

802.11k

This proposed standard is designed to add radio management data and reporting to access points. This information will be provided to other access points, switches, and client adaptors. The information is from layers 1 and 2. This will be a software upgrade to existing radios.

802.11l

Not used because the IEEE thought people might confuse the l with the i in 802.11i.

802.11m

802.11m is not a standard. The proposal for the "m" group is to go through the standards and perform maintenance. They will also be looking at rolling all of the various amendments to 802.11, such as 802.11a, 802.11b, and 802.11g, into a single standard.

802.11n

The 802.11n working group is looking into boosting the speeds of wireless LANs to 100 or even 320 Mbps. The main difference between this standard and the previous ones will be the requirement that the entire speed rating actually be useable. 100 Mbps will mean that the user will see data transfer at that rate, not the 50% rate that is normal now. Products supporting this standard are expected by early 2006.

802.11p

This is a proposed standard that gets little attention, but is very interesting. This is looking at high-speed automotive networks. These devices would operate at 6 Mbps up to 1000 feet while in motion. The idea is to provide information from highway side access points as the car zips by.

802.11q

The 802.1q standard defines VLAN bridges. These are to be used for creating virtual LANs within a bridged LAN infrastructure. The idea is to break up large networks into smaller parts so broadcast and multicast traffic will not overwhelm the limited available bandwidth.

802.11r

This standard will provide a common way to do Fast Secure Roaming. As discussed earlier, Cisco already has a proprietary version of this.

802.11s

It seems that interest in mesh networks rises and falls on a regular cycle. There are many proprietary methods. This standard seeks to unify these multiple methods.

802.11t

This is a standard for performance metrics, measurement methodologies, and test conditions.

802.11u

This group is working on a standard to allow 802.11-style networks to talk to other types of networks, such as cellular systems.

802.11v

This is another management standard. This one is intended to allow clients to adjust their power levels as needed. This will add to the management proposed for access points.

Cisco Proprietary Enhancements

Fast Secure Roaming

Fast Secure Roaming is a Cisco method used to allow authenticated clients to roam securely from one access point to another without any perceptible delay due to reassociation. This is required for real time applications such as VoWLAN. Handoff times are under the 150 ms typically required for this type of traffic. This is within a subnet. The device must support the Cisco Centralized Key Management (CCKM) protocol.

Layer 3 Mobility

Along with Fast Secure Roaming is Layer 3 Mobility. When the WDS is the WLSM, access points can be installed anywhere in a layer

3 network without using one specific subnet or VLAN throughout the wired switch infrastructure. Client devices use multipoint GRE (mGRE) tunnels to roam to access points assigned to different subnets. The client retains its IP address as it roams. Support for fast secure Layer 3 roaming is provided for Cisco or Cisco Compatible wireless LAN client devices by using the CCKM protocol.

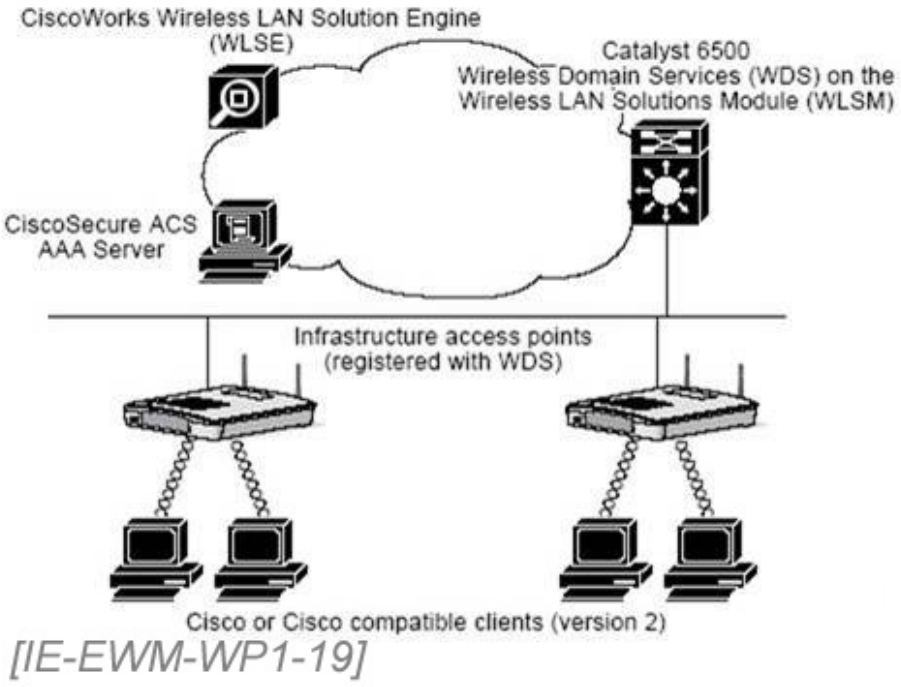


Figure 19. Components Required for Layer 3 Roaming

VoWLAN

VoWLAN seems to be an odd thing to put on the CCIE exam at this time. For example, a search of the Cisco web site using the term VoWLAN produces only three hits -- two of these are the exam blueprint. The other is an announcement that TI supports the Cisco Compatible Extensions for some of their devices. Even a Google search turns up "just" 33,200 pages. Including "Cisco" in the query narrows this to 9,120. Infonetics Research reports worldwide sales of 113,000 handsets last year. Consequently, there is not much to say on this subject right now, except that it is coming -- ready or not.

Cisco makes a suitable phone for this purpose in the Wireless IP Phone 7920.

Figure 20.

The major problem with using VoWLAN or voice over a wireless local area network is the lack of any quality of service (QoS)

mechanism built into wireless LANs. The 802.11e IEEE committee is working on this, but they have been for years. There is an interim proposal from the Wi-Fi Alliance called Wi-Fi Multimedia (WMM). Further, the bandwidth actually available on a wireless LAN is a little over half the theoretical rate. The 54 Mbps rate soon becomes 24.4 Mbps or less. This is not much throughput for data and voice to share. Symbol Technologies states that five phone calls will saturate an access point. One way around this is to use a dual radio unit such as the 1200 access point. Using this device, one radio can be used for data and the other for voice. Of course, the only available Cisco phone requires the 2.4 GHz frequency. Many client devices are still 802.11b/g units, so that may not work well at the present time.

Fast Secure Roaming is required for VoWLAN to work effectively. The primary use of Fast Secure Roaming is quick handoffs as users move from access point to access point. Without this, many applications cease to function. Fast Secure Roaming differs from standard roaming primarily in relation to the speed of the handoff. In standard roaming, which all access points support, the handoff time is around 200 ms. This is too slow for voice connections. Fast Secure Roaming makes the handoff in about 50 ms.

A WDS server and CCKM are required for this to function. This makes the Cisco implementation of Fast Secure Roaming a high cost solution. The standardized method from the IEEE is likely to be less expensive. As with most standards, it is difficult to say when it will appear on the market. This is definitely a changing area of development.

When the 7920 phone is used, Cisco recommends that the site survey procedure be changed. VoWLAN has more stringent requirements than data alone. For instance, they call for at least a 25 dB signal to noise ratio in all areas to be covered. The signal strength received at every point needs to be at least -67 dBm. There should be at least two access points within range of every user.

Security is an issue for wireless VoIP just as it is for data over a wireless network. Adding security overhead to the voice traffic slows the connection even more.

Conclusion

This tutorial has attempted to address the enterprise-related wireless mobility topics listed on the new CCIE R&S Written Exam blueprint. Because this is brand new, it remains to be seen exactly what Cisco will emphasize over time. Emphasis was placed on wireless security, because this is currently an active area of concern. In addition, SWAN is a major Cisco initiative.

[IE-EWM-WP1-F02]
[2005-03-04-01]